Beschreibung

Sicherheitsmodul zum Verschlüsseln eines Telefongesprächs

Die Erfindung betrifft ein Sicherheitsmodul zum Verschlüsseln eines Telefongesprächs zwischen einem oder mehreren ersten Telekommunikationsendgeräten in einem paketorientierten Datennetz und einem oder mehreren zweiten Telekommunikationsendgeräten in einem analogen und/oder digitalen Telefonnetz.

Aus dem Stand der Technik ist die Telefonie in IP-Netzen bekannt. Es existieren mittlerweile Standards, in denen die Signalisierung für die Telefonie in IP-Netzen festgelegt ist. Es handelt sich hierbei um den IETF Standard SIP und den ITU-Standard H.323, die auch als "Voice over IP" (VoIP) bezeichnet werden und hauptsächlich in LAN- oder WLAN-basierten Netzwerken Anwendung finden (LAN = Local Area Network, WLAN = Wireless Local Area Network). Bei der VoIP-Telefonie wurden bis heute hauptsächlich Sicherheitsaspekte in Bezug auf die Authentizität und Integrität von Kontroll- und Signalisierungsdaten betrachtet. In künftigen Lösungen wird neben der reinen Signalisierungssicherheit auch die Sicherheit der übertragenen Sprachdaten berücksichtigt. Zur Sicherung von Sprachdaten in IP-Netzen kommt beispielsweise das verschlüsselte Transportprotokoll SRTP (SRTP = Secure Real Time Transport Protocol; siehe Dokument [1]) in Betracht.

Mit den derzeitigen Sicherheitslösungen wird jedoch nur eine Sicherung von Sprachdaten in paketorientierten Netzwerken gewährleistet. Es existieren zwar auch Sicherheitslösungen für die Telefonie in öffentlichen Telefonnetzen, jedoch gibt es bis heute keine Möglichkeit, Telefongespräche von einem paketorientierten Netz zu einem öffentlichen Telefonnetz verschlüsselt durchzuführen.

Aufgabe der Erfindung ist es deshalb, ein Sicherheitsmodul zum Verschlüsseln eines Telefongesprächs zu schaffen, welches

eine Verschlüsselung der Sprachdaten in einem heterogenen Netzwerk umfassend ein paketorientiertes Datennetz und ein Telefonnetz ermöglicht.

Diese Aufgabe wird durch die unabhängigen Patentansprüche gelöst. Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen definiert.

Das erfindungsgemäße Sicherheitsmodul dient zum Verschlüsseln eines Telefongesprächs zwischen einem oder mehreren ersten Telekommunikationsendgeräten in einem paketorientierten Datennetz und einem oder mehreren zweiten Telekommunikationsendgeräten in einem analogen und/oder digitalen Telefonnetz, wobei im paketorientierten Netz Datenpakete mittels eines verschlüsselten Transportprotokolls transportiert werden und die Schlüssel für das verschlüsselte Transportprotokoll mittels eines Schlüssel-Austausch-Protokolls ausgetauscht werden. Im Folgenden ist unter einem Telefonnetz jede Art von öffentlichem PSTN-Netz (PSTN = Public Switched Telephone Network) zu verstehen, wobei es sich sowohl um ein analoges als auch um ein digitales Telefonnetz handeln kann. Das paketorientierte Netz und das Telefonnetz sind hierbei über einen Zugangsrechner miteinander verbunden und das Sicherheitsmodul kann bei einem Telefongespräch in einer Verbindungsleitung an einem ersten oder zweiten Telekommunikationsendgerät zwischengeschaltet werden. Der Begriff "Verbindungsleitung" ist hierbei allgemein zu verstehen, es kann sich sowohl um eine drahtgebundene als auch um eine drahtlose Verbindung an dem entsprechenden Telekommunikationsendgerät handeln.

Das erfindungsgemäße Sicherheitsmodul umfasst eine Protokollverarbeitungseinrichtung, welche Nachrichten des Schlüssel-Austausch-Protokolls sowie mittels des verschlüsselten Transportprotokolls transportierte Datenpakete verarbeitet, wenn das Sicherheitsmodul bei einem Telefongespräch in eine Verbindungsleitung an einem ersten oder zweiten Telekommunikationsendgerät zwischengeschaltet ist. Aufgabe der Protokollver-

arbeitungseinrichtung ist es, Sprachsignale, die an dem entsprechenden Telekommunikationsendgerät erzeugt werden, in Datenpakete zum Transport über das verschlüsselte Transport-Protokoll umzuwandeln und an dem Sicherheitsmodul ankommende Datenpakete, die über das verschlüsselte Transportprotokoll transportiert werden, in Sprachsignale umzuwandeln.

Das Sicherheitsmodul umfasst ferner eine Modemverbindungseinheit, welche immer dann zum Einsatz kommt, wenn das Sicherheitsmodul in einer Verbindungsleitung an einem zweiten Telekommunikationsendgerät zwischengeschaltet ist. In diesem Fall baut die Modemverbindungseinheit bei einem Telefongespräch eine Modemverbindung zwischen dem zweiten Telekommunikationsendgerät und dem Zugangsrechner und/oder einem weiteren zweiten Telekommunikationsendgerät auf, wobei über die Modemverbindung Datenpakete mittels des verschlüsselten Transportprotokolls sowie Nachrichten des Schlüssel-Austausch-Protokolls transportiert werden. Vorzugsweise läuft über die Modemverbindung eine PPP-Verbindung (PPP = Point to Point Protocol), mit der die Datenpakete des Transportprotokolls sowie die Nachrichten des Schlüssel-Austauschs-Protokolls transportiert werden. Durch die Modemverbindungseinheit im Sicherheitsmodul wird somit eine Übertragung von Verschlüsselungstechnologien aus paketorientierten Netzwerken in öffentliche Telefonnetze realisiert. Dies ist möglich, da Modemverbindungen heutzutage ausreichende Bandbreite bzw. Übertragungsraten zur Übertragung von Echtzeit-Mediendatenpaketen aufweisen.

In einer besonders bevorzugten Ausführungsform wird als verschlüsseltes Transportprotokoll SRTP (siehe Dokument [1]) verwendet. Für den Austausch der Schlüssel, die in dem verschlüsselten Transportprotokoll eingesetzt werden, wird vorzugsweise das Schlüssel-Autausch-Protokoll MIKEY (= Multimedia Internet KEYing) eingesetzt. MIKEY ist derzeit ein Draft bei der IETF, der in absehbarer Zeit zum Standard erklärt werden wird.

In einer weiteren Ausführungsform des Sicherheitsmoduls werden bei einem Telefongespräch Nachrichten des Schlüssel-Austausch-Protokolls über das aus dem Stand der Technik bekannte SIP-Protokoll (SIP = Session Initiation Protocol) transportiert, wobei die Protokollverarbeitungseinrichtung des Sicherheitsmoduls derart ausgestaltet ist, dass sie dieses Protokoll verarbeiten kann.

Das Telefonnetz, in dem das erfindungsgemäße Sicherheitsmodul zum Einsatz kommt, ist beispielsweise ein digitales ISDN-Netz. Vorzugsweise baut die Modem-Verbindungseinheit dabei eine Modemverbindung über den B-Kanal im ISDN-Netz auf. Bei dem paketorientierten Netz handelt es sich vorzugsweise um ein IP-basiertes Datennetz, insbesondere ein LAN-Netz. Die Modemverbindungseinheit stellt vorzugsweise eine Modemverbindung nach dem V90 und/oder V92-Standard her, wobei dieser Standard ausreichende Bandbreiten bzw. Übertragungsraten für die Übermittlung von Datenpaketen aus paketorientierten Netzen bereitstellt.

In einer Variante der Erfindung wird das Sicherheitsmodul für Telefone mit einem Verbindungskabel zwischen Telefonapparat und Telefonhörer verwendet, wobei das Sicherheitsmodul derart ausgestaltet ist, dass es in dem Verbindungskabel zwischengeschaltet wird.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der beigefügten Zeichnung beschrieben.

Es zeigt

Figur 1 die schematische Darstellung eines heterogenen Netzwerks, in dem das erfindungsgemäße Sicherheitsmodul zur Verschlüsselung von Sprachsignalen verwendet wird.

Das in Figur 1 gezeigte heterogene Netzwerk umfasst zum einen ein IP-basiertes lokales Netzwerk LAN (LAN = Local Area Network) sowie ein öffentliches TDM-Telefonnetz (TDM = Time Division Multiplexing). Bei dem TDM-Netz handelt es sich um ein digitales Netz, wobei jedoch zur Übertragung von gesprochener Sprache ein gesonderter analoger Sprachkanal verwendet wird. Das LAN- und das TDM-Netz sind über ein Gateway G miteinander verbunden. Das Gateway dient dazu, im LAN-Netz übertragene IP-Datenpakete zur Weiterleitung im TDM-Netz sowie Daten aus dem TDM-Netz zur Weiterleitung im LAN-Netz entsprechend zu modifizieren.

Im LAN-Netz befinden sich zwei sogenannte VoIP-Clients VoIP-C, welche das Telefonieren über paketorientierte Netze ermöglichen. Beim Telefonieren über "Voice over IP" können die dem Fachmann hinlänglich bekannten Standards SIP oder H.323 zur Signalisierung von Sprachnachrichten verwendet werden. Der untere VoIP-Client in Fig. 1 ist ein Telefon, mit dem der Aufbau einer verschlüsselten Telefonverbindung beabsichtigt ist. Deshalb ist zwischen dem Hörer des Telefons und dem eigentlichen Telefonapparat in der entsprechenden Verbindungsleitung das erfindungsgemäße Sicherheitsmodul SM zwischengeschaltet.

In dem TDM-Netz der Figur 1 sind beispielhaft zwei TDM-Clients TDM-C in Form von Telefonen gezeigt, mit denen ebenfalls verschlüsselte Telefongespräche geführt werden können. Deshalb ist auch bei diesen Telefonen zwischen dem Hörer und dem eigentlichen Telefonapparat in der Verbindungsleitung das erfindungsgemäße Sicherheitsmodul SM zwischengeschaltet.

Die aus dem Stand der Technik bekannten Sicherheitsmodule ermöglichen ein Verschlüsseln des Telefongesprächs nur innerhalb des TDM-Netzes, wobei jeder Telefongesprächsteilnehmer zum Aufbau einer verschlüsselten Telefonverbindung durch den Druck auf eine Taste an seinem Sicherheitsmodul jeweils einen Schlüssel erzeugt, der über ein proprietäres Signalisierungs-

protokoll zwischen den Telefonapparaten der Gesprächsteilnehmer ausgetauscht wird. Schließlich werden an Displays, die in den Sicherheitsmodulen integriert sind, jeweils Zahlenkombinationen angezeigt, welche sich die Gesprächsteilnehmer gegenseitig über die Telefonverbindung durchsagen. Sollten die Zahlenkombinationen übereinstimmen, kann davon ausgegangen werden, dass die Verbindung von keinem Dritten abgehört wird, so dass mit Hilfe der ausgetauschten Schlüssel schließlich die verschlüsselte Datenübertragung erfolgt, wobei hierzu wiederum ein proprietäres Protokoll verwendet wird. Experimente haben gezeigt, dass mit den herkömmlichen Sicherheitsmodulen keine verschlüsselten Telefongespräche zwischen einem Telefon in einem paketorientierten Netz und einem Telefon in einem TDM-Netz geführt werden können. Dies resultiert daher, dass in paketorientierten Netzen die Daten asynchron übertragen werden, was zu Bandbreitenschwankungen (auch als "Jitter" bezeichnet) führen kann, die von herkömmlichen Sicherheitsmodulen nicht verarbeitet werden können. Ebenso führen in paketorientierten Netzen auftretende Datenpaketverluste bei herkömmlichen Sicherheitsmodulen zu Problemen.

Das Sicherheitsmodul gemäß der hier beschriebenen Ausführungsform löst dieses Problem dadurch, dass es aus der IP-Welt bekannte Protokolle zum Verschlüsseln von Daten in einem normalen öffentlichen TDM-Netz verarbeiten kann. Hierzu ist in dem Sicherheitsmodul eine Protokollverarbeitungseinrichtung vorgesehen, welche das verschlüsselte Transportprotokoll SRTP (SRTP = Secure Real Time Protocol) verarbeiten kann. Dieses Protokoll wird voraussichtlich zukünftig als Standard zur verschlüsselten Übertragung von Medien-Daten verwendet. Darüber hinaus kann die Protokollverarbeitungseinrichtung das Schlüssel-Austausch-Protokoll MIKEY verarbeiten. Mit diesem Protokoll werden Schlüssel erzeugt und zwischen den Clients bzw. Telefonen im heterogenen Netz der Fig. 1 ausgetauscht. Die Schlüssel werden hierbei von dem Transportprotokoll SRTP zur verschlüsselten Übertragung der Datenpakete mittels SRTP verwendet. Die Protokollverarbeitungseinrichtung ermöglicht

unter anderem die verschlüsselte Telefonie zwischen VoIP-Clients im LAN-Netz. Dies ist in Figur 1 mit den Doppelpfeilen MIKEY-KM (KM steht für Key Management) und SRTP-MS (MS steht für Media Security) dargestellt.

Zum Aufbau einer verschlüsselten Telefonverbindung zwischen Teilnehmern im TDM-Netz bzw. zwischen einem Teilnehmer im LAN-Netz und einem Teilnehmer im TDM-Netz weist das Sicherheitsmodul SM eine Modemverbindungseinheit auf. Diese Modemverbindungseinheit stellt bei einem Telefongespräch eines Teilnehmers im TDM-Netz mit einem Teilnehmer im LAN-Netz eine Modemverbindung über einen Sprachkanal im TDM-Netzes zu dem Gateway G her. Vorzugsweise handelt es sich hier um eine V92 Modemverbindung, mit der Daten mit 56 kbit/s downstream und 48 kbit/s upstream übertragen werden können. Über diese Verbindung wird eine weitere Verbindung mittels des PPP-Protokolls (PPP = Point to Point Protocol) zur Verfügung gestellt, wobei über letztere Daten im Schlüssel-Austausch-Protokoll MIKEY bzw. im SRTP-Protokoll transportiert werden. Da diese Protokolle von der Protokollverarbeitungseinrichtung im Sicherheitsmodul SM verarbeitet werden können, wird somit eine Migration der Protokolle aus dem LAN-Netz in das TDM-Netz ermöglicht.

Die MIKEY-Nachrichten werden im LAN-Netz beispielsweise über das SIP-Protokoll transportiert. Im Gateway können die Inhalte der MIKEY-Nachrichten dann aus der SIP-Nachricht herausgeschnitten und in den PPP-Tunnel eingefügt werden. Es wäre jedoch auch denkbar, dass das Gateway die SIP-Nachrichten einfach an den PPP-Tunnel weiterschickt, ohne die MIKEY-Nachrichten herauszuschneiden. In einem solchen Fall muss die Protokollverarbeitungseinrichtung des Sicherheitsmoduls SM das SIP-Protokoll verarbeiten können. Somit ist auch eine Lösung denkbar, bei dem das Sicherheitsmodul SM als SIP-Endpunkt fungiert. In Bezug auf die Daten, die über das SRTP-Protokoll transportiert werden, übernimmt das Gateway G lediglich eine Weiterleitungsfunktion und verändert die Daten

nicht. Die gilt auch für die eigentlichen Schlüssel-Austausch-Daten in Form von MIKEY-Nachrichten. Bei Bedarf kann das Gateway jedoch auch als vertrauenswürdige Komponente in die Verbindung einbezogen werden, um so z.B. "Lawful Interception" zu ermöglichen.

Durch die Pfeile im unteren Bereich der Figur 1 wird nochmals der erfindungsgemäße Mechanismus verdeutlicht. Durch den mit p-IP bezeichneten Doppelpfeil (p-IP = plain IP) wird hervorgehoben, dass zum einen eine rein IP-basierte verschlüsselte Datenübertragung zwischen einem VoIP-Client VoIP-C und dem Gateway G verwendet wird. Demgegenüber wird zwischen dem Gateway G und einem TDM-Client TDM-C zum verschlüsselten Datentransport eine Modemverbindung verwendet, über welche das PPP-Protokoll läuft, mit dem wiederum IP-Datenpakete transportiert werden. Dies wird durch den Doppelpfeil IP-PPP-TDM verdeutlicht. Trotz dieser unterschiedlichen Verbindungsmechanismen wird zwischen einem Client im LAN-Netz und einem Client im TDM-Netz eine Ende-zu-Ende-Verschlüsselung mittels des Schlüssel-Austausch-Protokolls MIKEY und des SRTP-Transport-Protokolls SRTP erreicht. Dies wird durch die mit MIKEY-KM und SRTP-MS bezeichneten Doppelpfeile hervorgehoben.

Mit dem erfindungsgemäßen Sicherheitsmodul wird somit auf einfache Weise die Übertragung von aus der IP-Welt bekannten Verschlüsselungsprotokollen in ein öffentliches Telefonnetz ermöglicht. Dies wird durch eine Modemverbindung gewährleistet, welche aufgrund ihrer heutzutage möglichen Bandbreiten bzw. Übertragungsraten den Transport von Echtzeit-Datenpaketen und Signalisierungsnachrichten aus der IP-Welt ermöglicht.

Literaturverzeichnis:

[1] Internet Draft: The Secure Real-time Transport Protocol; Baugher, McGrew, Oran, Blom, Carrara, Naslund, Norrman; Work in Progress; http://search.ietf.org/internet-drafts/draft-ietf-avt-srtp-09.txt

[2] Internet Draft: MIKEY: Multimedia Internet KEYing; J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman; Work in Progress; http://search.ietf.org/internet-drafts/draft-ietf-msec-mikey-07.txt

Patentansprüche

1. Sicherheitsmodul zum Verschlüsseln eines Telefongesprächs zwischen einem oder mehreren ersten Telekommunikationsendgeräten (VoIP-C) in einem paketorientierten Datennetz (LAN) und einem oder mehreren zweiten Telekommunikationsendgeräten (TDM-C) in einem analogen und/oder digitalen Telefonnetz (TDM), wobei im paketorientierten Netz (LAN) Datenpakete mittels eines verschlüsselten Transportprotokolls transportiert werden und die Schlüssel für das verschlüsselte Transportprotokoll mittels eines Schlüssel-Austausch-Protokolls ausgetauscht werden, wobei das paketorientierte Netz (LAN) und das Telefonnetz (TDM) über einen Zugangsrechner (G) miteinander verbunden sind und wobei das Sicherheitsmodul (SM) bei einem Telefongespräch in eine Verbindungsleitung an einem ersten oder zweiten Telekommunikationsendgerät (VoIP-C; TDM-C) zwischengeschaltet werden kann, umfassend:
   - eine Protokollverarbeitungseinrichtung, welche Nachrichten des Schlüssel-Austausch-Protokolls sowie mittels des verschlüsselten Transportprotokolls transportierte Datenpakete verarbeitet, wenn das Sicherheitsmodul (SM) bei einem Telefongespräch in einer Verbindungsleitung an einem ersten oder zweiten Telekommunikationsendgerät (VoIP-C; TDM-C) zwischengeschaltet ist, wobei die Protokollverarbeitungseinrichtung an dem ersten oder zweiten Telekommunikationsendgerät (VoIP-C; TDM-C) erzeugte Sprachsignale in Datenpakete zum Transport über das verschlüsselte Transportprotokoll umwandelt und an dem Sicherheitsmodul ankommende Datenpakete, die über das verschlüsselte Transportprotokoll transportiert werden, in Sprachsignale umwandelt;
   - eine Modemverbindungseinheit, welche im Falle, wenn das Sicherheitsmodul (SM) in einer Verbindungsleitung an einem zweiten Telekommunikationsendgerät (TDM-C) zwischengeschaltet ist, bei einem Telefongespräch eine Modemverbindung zwischen dem zweiten Telekommunikations-

endgerät und dem Zugangsrechner (G) und/oder einem weiteren zweiten Telekommunikationsendgerät (TDM-C) aufbaut, wobei über die Modemverbindung die Datenpakete mittels des verschlüsselten Transportprotokolls sowie Nachrichten des Schlüssel-Austausch-Protokolls transportiert werden.

2. Sicherheitsmodul nach Anspruch 1, wobei über die Modemverbindung eine PPP-Verbindung läuft, über welche die Datenpakete mittels des verschlüsselten Transportprotokolls sowie Nachrichten des Schlüssel-Austausch-Protokolls transportiert werden.

3. Sicherheitsmodul nach Anspruch 1 oder 2, wobei das verschlüsselte Transportprotokoll SRTP (= Secure Real Time Protocol) ist.

4. Sicherheitsmodul nach einem der vorhergehenden Ansprüche, wobei das Schlüssel-Austausch-Protokoll MIKEY (= Multimedia Internet Keying) ist.

5. Sicherheitsmodul nach einem der vorhergehenden Ansprüche, wobei das Sicherheitsmodul (SM) derart ausgestaltet ist, dass bei einem Telefongespräch Nachrichten des Schlüssel-Austauch-Protokolls über das SIP-Protokoll (SIP = Session Initiation Protocol) transportiert werden, und die Protokollverarbeitungseinrichtung das SIP-Protokoll verarbeiten kann.

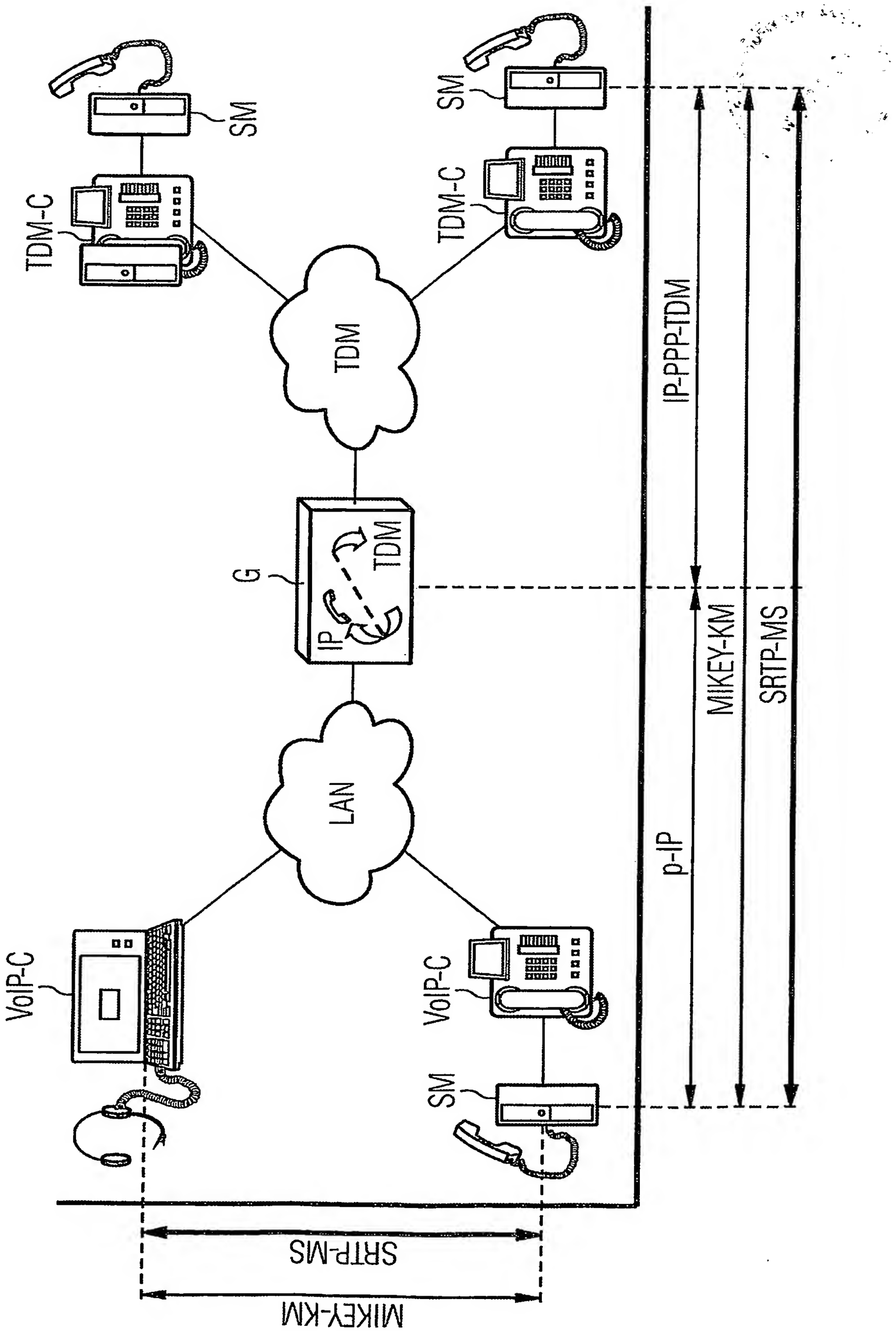
6. Sicherheitsmodul nach einem der vorhergehenden Ansprüche, bei dem das Telefonnetz (TDM) ein ISDN-Netz ist.

7. Sicherheitsmodul nach Anspruch 6, bei dem die Modemverbindungseinheit eine Modemverbindung über den B-Kanal im ISDN-Netz aufbauen kann.

8. Sicherheitsmodul nach einem der vorhergehenden Ansprüche, bei dem das paketorientierte Netz ein IP-basiertes Datennetz, insbesondere ein LAN-Netz (LAN = Local Area Network), ist.

9. Sicherheitsmodul nach einem der vorhergehenden Ansprüche, bei dem die Modemverbindungseinheit eine Modemverbindung nach dem V90 und/oder V92-Standard aufbauen kann.

10. Sicherheitsmodul nach einem der vorhergehenden Ansprüche, das für Telefone mit einem Verbindungskabel zwischen Telefonapparat und Telefonhörer eingesetzt wird, wobei das Sicherheitsmodul (SM) derart ausgestaltet ist, dass es in dem Verbindungskabel zwischengeschaltet wird.


SM
TDM-C
TDM
G
IP
TDM
LAN
VoIP-C
SM
TDM-C
VoIP-C
SM
p-IP
IP-PPP-TDM
MIKEY-KM
SRTP-MS
SRTP-MS
MIKEY-KM